

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Middle District of Georgia

United States of America
v.
MICHAEL RON DAVID KADAR

Case No.

3:17-MJ-4~~3:15-MJ-19~~RECEIVED
CLERK'S OFFICE

2017 APR 21 AM 11:55

U.S. DISTRICT COURT
MIDDLE DIST. OF GEORGIA
CLARK COUNTY*Defendant(s)*

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of January 3, 2017 in the county of Athens-Clarke in the
Middle District of Georgia, the defendant(s) violated:

*Code Section**Offense Description*

18 U.S.C. Section 875(c)
18 U.S.C. Section 1038(a)(1)(A)
18 U.S.C. Section 2261A(2)

Making Threatening Interstate and Foreign Communications
Conveying of False Information and Perpetuating a Hoax
Cyberstalking

This criminal complaint is based on these facts:

See attached affidavit

☒ Continued on the attached sheet.

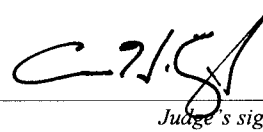
Complainant's signature

Jamie M. Hipkiss, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date:

April 21, 2017

Judge's signature

City and state:

Macon, Georgia

Charles H. Weigle, United States Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

1. I, Jamie M. Hipkiss, being duly sworn, depose and state the following:

2. I am a Special Agent with the U.S. Department of Justice, Federal Bureau of Investigation (FBI). I am currently assigned to the Atlanta Division, Athens Resident Agency (RA).

3. I have been employed as a Special Agent of the FBI since February 2013. Upon being hired as a Special Agent, I attended the FBI Academy in Quantico, Virginia, where I received extensive training on investigating various violations of federal law. While at the FBI Academy, I received specific training on using digital tools to conduct cyber investigations. Since then, I have participated in several criminal investigations involving cybercrimes. As part of those investigations, I have been involved in the execution of search warrants, arrest warrants, and interviews of defendants. Through my training at the FBI Academy, education and previous experiences in more than 9 years as a crime scene technician, police officer, and detective in Gwinnett County, Georgia, I have become familiar with the manner in which the Internet is used to perpetrate various crimes.

4. The information contained in this affidavit is based upon my personal knowledge and observations, interviews with persons, review of government and business records, and of records, reports, and information received from other law enforcement related sources. This affidavit is likewise based on reports and observations made by other law enforcement officers and the information obtained by other law enforcement officers. This affidavit is not intended to convey all the facts of the entire investigation, but rather to establish cause to support the request for a Federal criminal complaint.

5. This affidavit is made in support of a criminal complaint and arrest warrant alleging that Michael Ron David Kadar:

- a. Transmitted in interstate and foreign commerce any communication containing any threat to kidnap any person and any threat to injure the person of another; in violation of Title 18, United States Code, Section 875(c);¹
- b. Engaged in conduct with intent to convey false and misleading information under circumstances where such information may reasonably be believed and where such

¹ Title 18, United States Code, Section 875(c) provides: "Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both."

information indicates that an activity has taken, is taking, and will take place that would constitute a violation of Title 18, United States Code, Section 924(c)(1)(A),² in violation of Title 18, United State Code, Section 1038(a)(1)(A);³

- c. With the intent to injure, harass, and intimidate, used any interactive computer service and electronic communication service and electronic communication system of interstate commerce, and any other facility of interstate and foreign commerce to engage in a course of conduct that places a person in reasonable fear of the death of and serious bodily injury to, and causes, attempts to cause, and would be reasonably expected to cause substantial emotional distress to, that person, an immediate family member of that person, and a spouse and intimate partner of that person, in violation of Title 18, United States Code, Section 2261A(2);⁴ and

6. Kadar is a dual U.S.–Israeli citizen. During the criminal acts described herein, he resided in Ashkelon, Israel.

² Title 18, United States Code, Section 924(c)(1)(A) provides, in relevant part: “[A]ny person who, during and in relation to any crime of violence . . . for which the person may be prosecuted in a court of the United States, uses or carries a firearm, or who, in furtherance of any such crime, possesses a firearm, shall, in addition to the punishment provided for such crime of violence . . . be sentenced to a term of imprisonment”

³ Title 18, United States Code, Section 1038(a)(1)(A) provides, in relevant part: “Whoever engages in any conduct with intent to convey false or misleading information under circumstances where such information may reasonably be believed and where such information indicates that an activity has taken, is taking, or will take place that would constitute a violation of chapter . . . 40 [or] 44 . . . of this title . . . shall (A) be fined under this title or imprisoned not more than 5 years, or both[.]”

⁴ Title 18, United States Code, Section 2261A(2) provides, in relevant part: “Whoever — (2) with the intent to . . . injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, uses . . . interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that — (A) places that person in reasonable fear of the death of or serious bodily injury to [that person, an immediate family member of that person, or a spouse or intimate partner of that person]; or (B) causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to [that person, an immediate family member of that person, or a spouse or intimate partner of that person], shall be [imprisoned for not more than 5 years, in any other case, or both fined and imprisoned].”

The Investigation Begins: Three Athens, Georgia Swatting⁵ Calls in August 2015

7. On or about August 12, 2015, Barrow Elementary School in Athens, Georgia received a phone call from a “Restricted” number. When an employee answered the call, a computer-generated sounding voice stated, “we are in the school, we see children, we have guns, there will be a bloodbath, and something will detonate.”

8. On or about August 14, 2015, Timothy Road Elementary School in Athens, Georgia received a similar threat by telephone.

9. On or about August 19, 2015, Hilsman Middle School in Athens, Georgia received a similar threat in which the caller, in a “robotic” voice, said he was in the building and wanted to kill children.

10. In all three incidents, the schools were placed in lockdown while first responders searched the buildings to ensure they were safe. No suspicious persons or devices were encountered during the searches.

11. In August 2015, the FBI-Athens RA, the U.S. Attorney’s Office for the Middle District of Georgia, and the Computer Crime and Intellectual Property Section (CCIPS) of the Department of Justice opened an investigation into the aforementioned bomb threats.

12. On or about August 21, 2015, the FBI-Athens RA obtained from a service provider records and information related to the three aforementioned swatting calls, which identified a single email address (SWATTING EMAIL ADDRESS #1) and Voice over Internet Protocol (VoIP) service as being responsible for making all three calls. In addition, all three calls were placed using Internet Protocol (IP) addresses that reverted back to Israel.

13. Your affiant also learned that on or about August 12, 2015, the Knox County Sheriff’s Office (KCSO) responded to Gibbs High School in Corryton, Tennessee, regarding a threatening call. And on or about August 14, 2015, KCSO responded to a similar threatening call at Brickey McCloud Elementary School in Knoxville, Tennessee. During both incidents, first responders arrived, cleared the school, and determined both calls to be a hoax. Both swatting phone calls had been placed by SWATTING EMAIL ADDRESS #1.

14. Subsequent investigation by the FBI-Athens RA indicated that SWATTING EMAIL ADDRESS #1 was likely a compromised email address, as its password had been posted

⁵ Swatting is the act of tricking an emergency service into dispatching an emergency response based on the false report of an ongoing critical incident. The term derives from SWAT (Special Weapons and Tactics).

publically on the Internet, along with numerous other email addresses and passwords, combined with encouragement that the email addresses be used to perpetuate criminal activity.

15. In 2015, SWATTING EMAIL ADDRESS #1 was responsible for placing swatting calls to more than 90 victims (primarily schools) in more than 20 states and Canada. Many of the calls resulted in the temporary closure and evacuation or lockdown of the targeted facilities, and required law enforcement and emergency personnel to respond and clear the area. No actual explosives were found in relation to any of the calls.

Widespread Impact of the Swatting Phone Calls

16. As the investigation continued into the Fall and Winter of 2015, numerous swatting calls were made targeting victims in the Middle District of Georgia, including the following:

- a. On or about August 31, 2015 — Winterville Elementary School in Athens, Georgia;
- b. On or about September 25, 2015 — Cedar Shoals High School in Athens, Georgia;
- c. On or about October 20, 2015 — Clarke Central High School in Athens, Georgia;
- d. On or about December 10, 2015 — Whitehead Road Elementary School in Athens, Georgia; and
- e. On or about December 15, 2015 — Burney Harris Lyons Middle School in Athens, Georgia.

17. Numerous targets across the United States and the world were being victimized as well. For example, eleven swatting calls were made in Athens, Georgia between on or about August 12, 2015 and December 15, 2015 by six linked email accounts. Those same six accounts were responsible for more than 240 swatting victims (primarily schools) across the United States and Canada during that period. As a result, thousands of schoolchildren were evacuated.

2015 Swatting Calls to a Private Residence in Athens, Georgia

18. In addition to the swatting calls made to schools in Athens, Georgia, the FBI-Athens RA learned that multiple individuals residing at a private residence in Athens (ATHENS RESIDENCE #1) had been the victim of multiple swatting phone calls in December 2015.

19. On or about December 7, 2015, the Athens-Clarke County Dispatch received a call from a seemingly automated voice that reported numerous hostages, including possible children, were being held at gunpoint at ATHENS RESIDENCE #1. Police responded to the residence and

determined the two occupants were not in distress. While on scene, the phone rang again, and a digitized voice threatened that he was standing over a dead body next door and was ready to start shooting.

20. On or about December 8, 2015, the Athens-Clarke County police again responded to ATHENS RESIDENCE #1. One of the residents reported that someone had called and threatened, "Hello. If you do not answer me, I will kill you tonight. I am not so far away from you. Are there children in the house? Answer my question. Hello."

21. On or about December 9, 2015, a resident of ATHENS RESIDENCE #1 called the police to report that an ambulance had shown up at the home that evening. Emergency personnel reported they had received a phone call that someone was having a heart attack at ATHENS RESIDENCE #1.

Connection to Israeli IP Addresses Develops

22. During the investigation, agents for the FBI-Athens RA served more than 100 subpoenas, search warrants, and court orders to internet service providers, email providers, VPN services, and others in an effort to identify the individual who made the calls. The results of this voluminous legal process revealed several patterns. The swatting calls were typically made during the mornings Eastern Time and targeted schools, daycare centers, and airports. The perpetrator spoke through a text-to-voice service that disguised the caller's voice and placed the calls through a VoIP service. The terms "bloodbath" and "bomb" appeared repeatedly. The perpetrator accessed the VoIP service through proxy IPs and paid for services exclusively with virtual currency.

23. In addition, the perpetrator rarely used accounts for longer than a day or two, preferring to place numerous swatting calls in a short period and then abandon the account. The perpetrator also searched for news media reports following swatting phone calls. Moreover, a significant number of IP addresses that accessed the accounts used exclusively for swatting appeared to be located in Israel.

24. Because of the repeated connection to IP addresses located in Israel, in October 2015, the FBI-Athens RA, CCIPS, and the U.S. Attorney's Office for the Middle District of Georgia reached out to Israeli law enforcement in an effort to identify the perpetrator. Specifically, U.S. authorities sought the preservation of several IP addresses, including those linked to SWATting EMAIL ADDRESS #1 and numerous other accounts used for swatting calls, and the production of related records.

Israeli Authorities Open a Domestic Parallel Investigation

25. In late Summer or early Fall of 2016, Israeli authorities opened a domestic parallel investigation into related swatting activity.

26. Thereafter, law enforcement authorities from Israel, Australia, and New Zealand collaborated with the FBI-Athens RA, as it appeared that multiple countries had suffered similar threats. Law enforcement agencies from the four countries, including the Israeli Cyber Fusion Center of the Israeli National Police (INP), began to share the results of legal process obtained in their respective investigations.

January 3, 2017 Threat to Individual Victims at Private Residence in Athens, Georgia

27. On or about January 3, 2017, the University of Georgia Police Department in Athens, Georgia received a phone call that a home invasion was underway at ATHENS RESIDENCE #1, and one person had been shot in the chest, while three people were being held hostage. Athens-Clarke County Police responded to ATHENS RESIDENCE #1, where they determined that the residents were safe, but upset by the repeated threatening calls. The swatting call was placed through third party services that provide services such as VoIP, voice alteration, call recording, and “spoofing” the caller identification.

**Subsequent Investigation in Israel, and the
Re-Discovery of SWATTING EMAIL ADDRESS #1**

28. Israeli authorities, based on the IP addresses provided by the FBI-Athens RA, CCIPS, and the U.S. Attorney’s Office for the Middle District of Georgia, as well as their own subsequent investigation, identified a particular neighborhood in the city of Ashkelon, Israel, as the physical location where the IP addresses were serviced. Based on interviews with individuals who resided at these locations, Israeli authorities determined that the IP addresses were available as open, unprotected wireless networks.

29. Israeli authorities subsequently coordinated with the FBI regarding various means that the perpetrator might be accessing these IP addresses. In addition, a connection was discovered between the FBI-Athens RA case and an ongoing investigation of swatting calls against Jewish Community Centers (JCC), which was being pursued by the U.S. Attorney’s Office for the Middle District of Florida, FBI-Orlando RA, and the Civil Rights Division of the U.S. Department of Justice. Ultimately, FBI employees traveled to Israel to work with their Israeli counterparts in an effort to locate the perpetrator.

30. During surveillance of the neighborhood in Ashkelon, Israeli authorities observed a large parabolic antenna, which appeared to enable long-distance outdoor directional connections to wireless networks, physically connected to a particular apartment unit.

31. On or about March 23, 2017, the INP executed a search warrant at the apartment unit that had been identified with the large antenna. During this operation, INP took Michael Ron David Kadar and his father into custody.

32. INP searched Michael Kadar's bedroom and located a handwritten note containing SWATTING EMAIL ADDRESS #1 and what appeared to be the account's password. The search also identified a cable running from the parabolic antenna at the residence window to a network adapter connected to a laptop in Michael Kadar's bedroom. This device would have allowed Michael Kadar to access open Wi-Fi networks at other, distant locations.

33. INP seized the laptop located in Michael Kadar's bedroom, along with a USB flash drive connected to the laptop.

Preliminary Analysis of the USB Flash Drive

34. Preliminary forensic analysis of the USB flash drive attached to the laptop in Michael Kadar's bedroom revealed hundreds of recorded swatting calls, organized by date and geographic location, as well as media reports covering those swatting calls.

35. Among the hundreds of recorded swatting calls, there were recordings of the:

- a. August 12, 2015 swatting call related to Barrow Elementary School;
- b. August 14, 2015 swatting call related to Timothy Road Elementary School;
- c. August 19, 2015 swatting call related to Hilsman Middle School;
- d. August 31, 2015 swatting call related to Winterville Elementary School;
- e. September 25, 2015 swatting call related to Cedar Shoals High School;
- f. October 20, 2015 swatting call related to Clarke Central High School;
- g. December 7, 2015 swatting call related to ATHENS RESIDENCE #1;
- h. December 8, 2015 swatting call related to ATHENS RESIDENCE #1;
- i. December 9, 2015 swatting call related to ATHENS RESIDENCE #1;

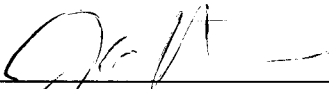
- j. December 10, 2015 swatting call related to Whitehead Road Elementary School;
- k. December 15, 2015 swatting call related to Burney Harris Lyons Middle School;
and
- l. January 3, 2017 swatting call related to ATHENS RESIDENCE #1.

36. In addition, the flash drive contained what appear to be advertisements offering swatting services for sale.

Submission of Probable Cause

37. Based on the above, your affiant respectfully submits that probable cause exists to believe that Michael Ron David Kadar has violated Title 18, Section 875(c) of the United States Code, in that it is probable to believe that he made threatening interstate communications; violated Title 18, Section 1038(a)(1)(A) of the United States Code, in that it is probable to believe he conveyed false information and perpetuated a hoax; and violated Title 18, Section 2261A(2) of the United States Code, in that it is probable to believe he committed cyberstalking.

Respectfully Submitted,



JAMIE M. HIPKISS
Special Agent
Federal Bureau of Investigation

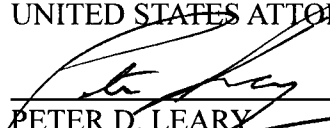
SUBSCRIBED and SWORN before me this 21st day of April, 2017



HONORABLE CHARLES H. WEIGLE
UNITED STATES MAGISTRATE JUDGE

REVIEWED AND APPROVED BY:

G.F. "PETE" PETERMAN, III
UNITED STATES ATTORNEY



PETER D. LEARY
Assistant United States Attorney
Georgia Bar Number 612045
United States Attorney's Office
Middle District of Georgia
Macon, Georgia 31202-1702
Telephone: (478) 752-3511

RYAN K. DICKEY
Senior Counsel
U.S. Department of Justice, Criminal Division
Computer Crime and Intellectual Property Section